



Attorney General Jon Bruning

NEWS RELEASE

FOR IMMEDIATE RELEASE

Thursday, April 8, 2010, 2:30 p.m.

Contact: Allen Forkner

402.471.2067

allen.forkner@nebraska.gov

Note: A sound bite on this topic will be available shortly at: <http://www.ago.ne.gov>

CONSUMER ALERT: Text Message Phishing Scam Targeting Bank Customers

LINCOLN – Attorney General Jon Bruning issued a warning today after Nebraskans in York, Polk, and Hamilton counties began randomly receiving text messages asking them to provide personal bank account information.

Text messages appearing to be from Cornerstone Bank informed consumers that their accounts had been compromised. They were then directed to dial a Lincoln-area phone number, where an automated phone system asked them to enter their account information, including PINs and security codes. Bank officials have told the Attorney General's Office that the messages did not come from Cornerstone Bank.

“Today's scam artists use the latest technology to prey on trusting Nebraskans,” Bruning said. “No matter how convincing they may appear, a bank will never contact you and ask for passwords or security numbers. If you have the slightest doubt, hang up and call the bank.”

Attempts to acquire personal information, called phishing, can leave victims with empty bank accounts or stolen their identities.

According one bank official, the text messages appear to have been sent to random people in the affected counties, regardless if they were Cornerstone Bank customers. This recent scam attempt is similar to a recent phishing attempt aimed at bank customers in Broken Bow. There, victims received an automated phone call asking them to punch in their account information to reactivate their accounts.

If you believe you may have been a victim of this phishing attempt, please call the Attorney General's Office at 800-727-6432 or visit our Web site at ago.ne.gov.

Tips to Recognize, Avoid Phone Phishing Attempts

- If you get a phone call that asks for personal or financial information, hang up. Legitimate companies don't ask for this information when they call you. If you are concerned about your account, contact the organization using a telephone number you know to be genuine.
- Area codes can mislead. Caller ID may appear to be from a legitimate business, but scammers use Voice Over Internet Protocol technology or they 'spoof' numbers that appear to be legitimate to present a false area code or phone number. If you need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card.
- If you believe your debit card information has been stolen, contact your bank and card issuing company immediately. If you report the card/ information lost or stolen and it has not been used within 2 business days, you are not liable for anything. If the card is used after two days, you are only responsible for \$50. If you report the fraud between the 2 days and 60 days you are liable for activity up to \$500. Any reports after 60 days of the first fraudulent use may leave you liable for all of the charges made on your card.
- If you believe you've been a victim, call the Consumer Protection Division to file your complaint or go online to ago.ne.gov and fill out the online consumer complaint form. If you have given personal or financial information out to a scammer, you should contact your credit card providers and bank immediately. Also, notify the three major credit bureaus that your information may have been stolen put fraud alerts on your credit.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Contact us for a free copy of the Identity Theft Repair Kit, which will walk victims through the steps necessary to safeguard their credit.
- While you can't entirely control whether you will become a victim of identity theft, you can take some steps to minimize your risk. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early if you order a free copy of your credit report periodically from any of the three major credit bureaus. See www.annualcreditreport.com for details on ordering a free annual credit report.

###